UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
FORT WAYNE DIVISION

Anthony Webster and **Mark Smith**, on behalf of themselves and all others similarly situated, Plaintiffs, v. **Bradford-Scott Data, LLC d/b/a Sharetec,** Defendant.	Case No. 1:24-cv-00117

DEFENDANT'S BRIEF IN SUPPORT OF ITS MOTION TO DISMISS AND MOTION TO STRIKE PLAINTIFFS' AMENDED CLASS ACTION COMPLAINT

Defendant Bradford-Scott Data, LLC d/b/a Sharetec ("Defendant" or "Bradford-Scott"), by and through its undersigned counsel, hereby submits this Brief in support of its Motion to Dismiss and Motion to Strike Plaintiffs Anthony Webster and Mark Smith's Amended Class Action Complaint pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(6), and 12(f).

I. Introduction

Plaintiffs Anthony Webster and Mark Smith (collectively, "Plaintiffs") have not been the victims of identity theft or any actual harm. There are no allegations in the Amended Class Action Complaint ("Amended Complaint") that cybercriminals used their personal information to commit fraud or in furtherance of any other type of nefarious scheme. Further, the Amended Complaint is silent as to whether Plaintiffs suffered any misuse, misappropriation, identity theft, fraud or any actual damages stemming from the criminal data security incident suffered by Defendant. Accordingly, Plaintiffs have not suffered any injuries-in-fact and do not have standing to bring this

putative class action lawsuit under Article III of the United States Constitution. The Court should dismiss the Amended Complaint pursuant to Federal Rule of Civil Procedure 12(b)(1) for lack of subject matter jurisdiction.

Even if Plaintiffs have standing to pursue this lawsuit, they failed to plead sufficient facts to state a claim for any of the causes of action asserted in the Amended Complaint. The Amended Complaint should therefore also be dismissed for failure to state a claim upon which relief can be granted pursuant to Rule 12(b)(6). Finally, if the Court does not dismiss the Amended Complaint, it should strike the immaterial and impertinent allegations concerning identity theft and general statistics about cybercrime that has nothing to do with the parties or facts of this case pursuant to Rule 12(f).

II. Relevant Factual Allegations[1]

Defendant Bradford-Scott Data, LLC d/b/a Sharetec is an Indiana-based company that is a technology and data service provider for credit unions across the country. Amended Compl. ¶¶ 10, 14. In July 2023, Defendant discovered it experienced a cyber incident, and through its thorough investigation, determined that certain documents may have been compromised (the "Data Security Incident"). *Id*. at ¶¶ 23 – 31. In February 2024, Defendant began notifying potentially affected individuals about the Data Security Incident. *Id*. at ¶ 33. Defendant is still unaware of any actual or attempted misuse of any of the affected information as a result of this Data Security Incident.

Plaintiff Anthony Webster is a citizen of Wyoming. *Id*. at ¶ 8. He is a former customer of StagePoint Federal Credit Union ("StagePoint"), which contracted with Defendant for technology

[1] For the purposes of this motion only, all well-pleaded facts of Plaintiffs' Amended Complaint are treated as true. However, Defendant does not admit the truth of any allegations in the Amended Complaint and cites them here solely for purposes of this motion.

and data services. *Id.* at ¶¶ 2, 46 – 47. Plaintiff Mark Smith is a citizen of Indiana. *Id*. at ¶ 9. He is a former customer of a credit union to which Defendant provided services. *Id*. at ¶ 63.

Plaintiffs brought this action on behalf of themselves and on behalf of a proposed putative nationwide class of "[a]ll individuals residing in the United States whose PII was compromised in the Data Breach discovered by Bradford-Scott in July 2023, including all those individuals who received notice of the breach." *Id*. at ¶ 98. Plaintiffs assert claims based on negligence, negligence *per se*, breach of implied contract, invasion of privacy, unjust enrichment, bailment, and seek injunctive relief. *Id.* at ¶ ¶ 108-190.

Plaintiff Anthony Webster alleges he received a notice letter in February 2024, stating that certain personally identifiable information ("PII") was potentially accessible in the Data Security Incident. *Id*. at ¶¶ 52 – 54. Plaintiff Mark Smith asserts he received a notice letter dated April 30, 2024. *Id*. at ¶ 67. Plaintiff Smith alleges that he has experienced an increase in spam calls, texts and/or emails, purportedly related to the Data Security Incident. *Id*. at ¶ 70. Plaintiffs, however, have not pled any facts in their Amended Complaint that suggest they suffered any tangible harm traceable to the Data Security Incident. Specifically, there are no facts in the Amended Complaint that show the Plaintiffs experienced identity theft, fraud, or any other concrete harm, and Plaintiffs do not have any valid damages.

III. Legal Argument

A. Plaintiffs' Claims should be Dismissed for Lack of Article III Standing

Plaintiffs failed to sufficiently plead any ***facts*** showing that they suffered concrete injuries-in-fact sufficient to give rise to standing under Article III of the United States Constitution. The Court should therefore dismiss the Amended Complaint in its entirety pursuant to the Federal Rule of Civil Procedure 12(b)(1) for lack of subject matter jurisdiction.

1. Plaintiffs Bear the Burden to Show Standing Exists

Article III limits the jurisdiction of federal courts to "cases" and "controversies." U.S. Const. art. III, § 2. To have standing under Article III, a plaintiff must show each of the following elements: (1) an injury-in-fact; (2) a traceable causal connection between the injury and the conduct complained of; and (3) that it is likely, as opposed to merely speculative, that the injury will be "redressed by a favorable decision." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). "Standing is an essential and unchanging part of the case-or-controversy requirement of Article III." *Id*. at 560.

"A case is properly dismissed for lack of subject matter jurisdiction when [a federal] court lacks the statutory or constitutional power to adjudicate the case." *Home Builders Ass'n of Miss., Inc. v. City of Madison*, 143 F.3d 1006, 1010 (5th Cir. 1998) (internal citation omitted). "As the party invoking federal jurisdiction, the plaintiffs bear the burden of demonstrating that they have standing." *TransUnion, LLC v. Ramirez*, 594 U.S. 413, 430–431 (2021). A plaintiff must demonstrate standing "with the manner and degree of evidence required at the successive stages of the litigation," including at the pleading stage. *Lujan*, 504 U.S. at 561.

2. Plaintiffs Must Show Injuries-in-Fact

To have standing to sue, a plaintiff must have suffered an injury-in-fact that is concrete, particularized, and actual or imminent, not merely conjectural or hypothetical. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 330 (2016); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013). "For an injury to be 'particularized,' it 'must affect the plaintiff in a personal and individual way.'" *Spokeo*, 578 U.S. at 330 – 331 (quoting *Lujan*, 504 U.S. at 560 n.1). As for concreteness, "[a] concrete injury must be *de facto*; that is, it must actually exist." *Id.* (internal citations and quotation marks omitted). In other words, it must be "real, and not abstract." *Id*. Because an injury-in-fact

cannot be conjectural or hypothetical, mere "[a]llegations of possible future injury are not sufficient." *Clapper*, 568 U.S. at 409.

3. Plaintiffs Do Not Have Article III Standing to Seek Damages

Plaintiffs fail to carry their burden of establishing standing to pursue this case under Article III. According to the allegations in the Amended Complaint, Plaintiffs have not suffered any actual injury, such as identity theft, actual misuse of their information, or economic harm. Because a plaintiff must have already suffered an injury-in-fact in order to have Article III standing in a case for damages, Plaintiffs' claims should be dismissed.

Plaintiffs only allege that they "suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft…"Amended Compl. ¶ 60. A "risk" of identity theft is not identity theft or fraud. Simply put, Plaintiffs failed to allege any risk of future harm that can confer standing.

In *TransUnion*, the Supreme Court clarified the standard that a plaintiff must meet when seeking to establish standing on the basis of a potential future injury. In assessing whether the risk of future harm can constitute an injury-in-fact under Article III, the Supreme Court distinguished between claims seeking injunctive relief and claims seeking monetary damages, finding that in a suit for damages, the mere risk of future harm, without more, cannot qualify as a concrete harm sufficient to establish standing. *TransUnion*, 594 U.S. 413. Instead, the Court held that a plaintiff must show that the harm actually materialized. *Id*.

In reaching its conclusion, the Supreme Court likened the statutory violation underlying the *TransUnion* plaintiffs' claimed injuries to the common law tort of defamation and explained that "there is 'no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury.'" *Id.* at 434 (quoting *Owner-*

Operator Indep. Drivers Ass'n, Inc. v. U.S. Dep't of Transp., 879 F.3d 339, 344 (D.C. Cir. 2018)). In rejecting the argument that risk of future disclosure of a credit report could serve as a concrete harm constituting an injury-in-fact satisfying Article III, the Supreme Court agreed with the argument TransUnion advanced:

> [I]f an individual is exposed to a risk of future harm, time will eventually reveal whether the risk materializes in the form of actual harm. If the risk of future harm materializes and the individual suffers a concrete harm, then the harm itself, and not the pre-existing risk, will constitute a basis for the person's injury and for damages. If the risk of future harm does *not* materialize, then the individual cannot establish a concrete harm sufficient for standing[.]

TransUnion, 594 U.S. at 436 (emphasis in original). Similarly, in this case, Plaintiffs alleged that their personal information may have been accessible without authorization during the Data Security Incident, but no allegations of concrete injury exist until it can be proven that information was actually misused in some way. Here, Plaintiffs have not asserted any allegations of actual misuse.

As one decision noted, "[g]iven the holding in *TransUnion*, it is far from clear that any case finding a concrete injury based merely on an abstract risk of future identity theft following a data breach is still good law, at least with respect to a claim for damages." *Legg v. Leaders Life Ins. Co.*, 574 F.Supp.3d 985, 993 (W.D. Okla. 2021); *see also Ewing v. MED-1 Solutions, LLC*, 24 F.4th 1146, 1152 (7th Cir. 2022) ("TransUnion makes clear that a risk of future harm, without more, is insufficiently concrete to permit standing to sue for monetary damages in federal court"). Indeed, in data privacy class actions since *TransUnion*, courts have found plaintiffs lack Article III standing when seeking damages where their purported injuries-in-fact consist of the risk of future of harm. *See Legg*, 574 F.Supp.3d at 993 (dismissing case where "Plaintiff only pleads facts showing that there is a non-imminent risk of possible future injury following the data breach,

[which] is not sufficient to confer standing"); *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig*., No. 19-2904, 2021 WL 5937742, at *10 (D.N.J. Dec. 16, 2021) (dismissing claims brought by plaintiffs alleging risk of future identity theft who "fail to account for . . . the Supreme Court's recent admonition that an unmaterialized risk of future of harm cannot confer standing in a claim for damages").

The Supreme Court's Article III standing analysis in *TransUnion* comports with Seventh Circuit precedent. In *Pierre*, a consumer brought a class action lawsuit against a debt collector that sent a letter seeking payment on a debt where the statute of limitations had already run. *Pierre v. Midland Credit Mgmt., Inc*., 29 F.4th 934, 936 (7th Cir. 2022). The consumer-plaintiff argued the letter was deceptive and "created a risk" that she might make a payment, even though she took no action to her detriment. *Id*. at 939. The court reasoned that the steps the plaintiff took in response to the letter – seeking legal counsel, calling the debt collector, and experiencing worry and confusion – were not concrete, legally cognizable harms, and held the plaintiff did not have Article III standing. *Id*. at 940.

In *Kim*, McDonalds USA suffered a data breach wherein third-party cybercriminals stole McDelivery users' delivery addresses, phone numbers, and email addresses. *Kim v. McDonald's USA, LLC*, No. 21-cv-05287, 2022 WL 4482826, *1 (N.D. Ill. Sep. 27, 2022). The plaintiffs alleged they experienced increased spam emails and unauthorized email log-in attempts, and that they suffered an increased risk of identity theft and phishing scams, lost time, anxiety, emotional distress, loss of privacy, and incurred expenses dealing with the alleged consequences of the data breach. *Id.* at *3. The court reasoned that plaintiffs' injury allegations were too attenuated and speculative, and any future harm rested on a "highly attenuated chain of possibilities." *Id*. at 4 (citing to *Clapper*, 568 U.S. at 413). The court concluded that plaintiffs failed to plausibly allege

that the future harms – identity theft and falling victim to phishing scams – were "certainly impending," concluding that the plaintiffs lacked Article III standing. *Id.* at *4.

Like the plaintiffs in *Pierre* and *Kim*, here Plaintiffs fail to allege a present, concrete injury or other already-materialized harm stemming from Defendant's Data Security Incident. Plaintiffs' allegations based on the risk of future harm, standing alone, are insufficient to confer Article III standing.

4. Mitigation Efforts do not Establish an Injury-in-Fact under Article III

Attempting to allege some type of redressable injury, Plaintiffs also claim they "anticipate[]" spending time and money on mitigation efforts related to the risk of future identity theft. Amended Compl. ¶¶ 61, 72, 128. Plaintiffs generally allege that they have suffered and will continue to suffer monetary loss, loss of time and productivity from mitigation efforts, and economic harm. *Id.* at ¶¶ 55, 61, 68, 128. However, they have not included any supporting detail or factual allegations regarding how they incurred the claimed economic losses or how they lost time through these purported mitigation efforts.

Even if Plaintiffs had included such specifics, however, a plaintiff cannot "manufacture standing" simply by "incur[ing] certain costs as a reasonable reaction to a risk of harm." *Clapper*, 568 U.S. at 416. In *Kim*, the court rejected plaintiffs' mitigation arguments, finding that plaintiffs "cannot rely on their time and money spent in response to fears that are too speculative to support standing under Article III" when the fear of future harm was not certainly impending. *Kim*, 2022 WL 4482826, *6. A number of courts have reached this conclusion in data breach cases. *See*, *e.g.*, *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021) (noting the plaintiff "cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft"); *Legg*, 574 F. Supp. 3d 985, 994 ("Thus, while it may have

been reasonable to take some steps to mitigate the risks associated with the data breach, those actions cannot create a concrete injury" sufficient to confer standing to seek damages).

Here, where the harm of identity theft failed to materialize, Plaintiffs cannot use mitigation efforts to create Article III standing where it does not already exist.

5. Plaintiffs Cannot Show Standing Through Alleged Diminution in Value of Personal Information

Plaintiffs also argue that they suffered injuries in the form of damages to and diminution in the value of their PII. Amended Compl. ¶¶ 59, 69, 75. Plaintiffs have not—and cannot—offer any factual support for this argument.

In *Gubal*a, the Seventh Circuit evaluated whether a former subscriber of Time Warner suffered injuries sufficient to confer Article III standing after Time Warner Cable maintained a copy of the plaintiff's personal information for years after plaintiff cancelled his subscription. *Gubala v. Time Warner Cable, Inc*., 846 F.3d 909, 910 (7th Cir. 2017). The court noted the plaintiff had not alleged his information was leaked, that he suffered any financial harm, or even that the information was at risk of being leaked while in Time Warner's possession. *Id*. at 910 – 911. The court reasoned the plaintiff had not alleged any concrete or plausible risk of harm from Time Warner's possession of his information. *Id*. The plaintiff further argued that his personal information had economic value and Time Warner's retention of his information "deprived" him of the full value of his transaction. *Id.* at 913. The Seventh Circuit explicitly rejected plaintiff's claim, characterizing his argument for the loss in value of his information as "gibberish," and concluded the plaintiff had not suffered any concrete injuries to confer Article III standing. *Id*.

The decisions that have accepted diminution in value of personal information to establish standing "involved circumstances where the defendants collected information that was itself monetized and used for commercial purposes." *In re Am. Med. Collection Agency*, 2021 WL

5937742, at *10. "The [Complaint] here contains no similar allegation. Absent such circumstances, there is no loss of value in the information sufficient to state a concrete injury." *Id.*; *see also Green v. eBay, Inc.*, No. 14-1688, 2015 WL 2066531, n.59 (E.D. La. May 4, 2015) ("Plaintiff has failed to allege facts indicating how the value of his personal information has decreased as a result of the Data Breach"). Similarly, standing has not been found in cases like this, where a plaintiff did not "explain how the hackers' possession of [her PII] has diminished its value, nor [did] she assert that she would ever actually sell her own personal information." *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 533–34 (D. Md. 2016). Plaintiffs here similarly offer no factual support for their conclusory argument that their information lost value. Accordingly, they cannot rely on this theory to establish standing.

6. Spam Messages Do Not Constitute an Injury-in-Fact

Plaintiff Smith alleges that he experienced an increase in spam emails, text messages, and phone calls as a result of the Data Security Incident. Amended Compl. ¶ 70. Numerous courts have determined that increased spam messages are insufficient to constitute an injury-in-fact for Article III standing in data breach cases. *See, e.g., Pulliam v. West Technology Group, LLC*, 8:23-cv-159, 2024 WL 356777, at *10 (D. Neb. Jan. 19, 2024) (analyzing plaintiffs' allegations of harm in a data breach and determining that an increase in spam messages is not a cognizable harm for Article III standing); *McCombs v. Delta Grp. Electronics, Inc.*, 676 F. Supp. 3d 1064, 1074 (D. N.M. 2023) (rejecting plaintiff's argument that increased spam communications after the defendant's data breach were a concrete harm because the plaintiff had not plausibly asserted a nexus between the incident and the spam communications); *In re Illuminate Educ. Data Sec. Incident Litig.*, No. 22-1164, 2023 WL 3158954, at *3 (C.D. Cal. Apr. 19, 2023) (determining the plaintiff's "receipt of spam, absent any other injury, is insufficient to establish an injury for the

purposes of standing"); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1051 (N.D. Cal. 2022) (reasoning that the plaintiffs' receipt of spam emails, without more, does not constitute an injury-in-fact for Article III standing purposes); *Blood v. Labette County Medical Center*, 5:22-cv-04036, 2022 WL 11745549, at *6 (D. Kan. Oct. 20, 2022) (finding that spam calls, texts, and emails do not constitute an injury-in-fact for standing); *Legg*, 574 F.Supp.3d at 993 (determining plaintiff's "receipt of phishing emails…does not 'plausibly suggest' that any actual misuse" of her information occurred, concluding plaintiff failed to establish Article III standing).

Plaintiffs' Amended Complaint here offers no basis to reach a different conclusion on this point than did the numerous courts cited above. Plaintiff Smith claims that he has experienced an increase in spam calls, texts, "and/or" emails which he believes was caused by the security incident "upon information and belief." Amended Compl. ¶ 70. Not only is Smith curiously unaware of whether the increase of spam took the form calls, texts, emails, or some combination thereof, he offers no further information as to the nature of this supposed increase, whether he was receiving such contact before, etc. He also seemingly admits that the information involved in the security incident would ***not*** be sufficient to result in an increase in calls, and that information like his phone number or email address would have come from other sources. *Id.* That is, he inherently admits a lack of traceability with respect to the supposed increase in spam. Therefore, Smith's allegations on this front fall short of establishing his own standing. Further, Plaintiff Webster does not even allege in conclusory terms such an increase in spam communications, and therefore cannot rely on this as a basis for establishing standing to bring his own claims.

B. Plaintiffs Failed to State a Valid Claim upon which Relief can be Granted

To survive a Rule 12(b)(6) motion, a complaint must "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atlantic Corp. v. Twombly*,

550 U.S. 544, 570 (2009)). A complaint must include "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Lincoln v. Turner*, 874 F.3d 833, 839 (5th Cir. 2017) (citing *Twombly*, 550 U.S. at 555). "Nor does a complaint suffice if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557). "Factual allegations must be enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555. "[W]hen the allegations in a complaint, however true, could not raise a claim of entitlement to relief, 'this basic deficiency should . . . be exposed at the point of minimum expenditure of time and money by the parties and the court.'" *Cuvillier v. Taylor*, 503 F.3d 397, 401 (5th Cir. 2007) (quoting *Twombly*, 550 U.S. at 558). Plaintiffs failed to plead sufficient facts to support any of the causes of action set forth in the Amended Complaint.

1. Plaintiffs Fail to State a Claim for Negligence

a. Indiana Does Not Recognize a Duty to Protect Information

Under Indiana law, the elements for a negligence cause of action are: (1) a duty owed to plaintiff by defendant, (2) breach of duty by allowing conduct to fall below the applicable standard of care, and (3) a compensable injury proximately caused by defendant's breach of duty. *Bader v. Johnson*, 732 N.E.2d 1212, 1216–17 (Ind. 2000). Damages are an essential element in a tort action. *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 635 (7th Cir. 2007) (dismissing plaintiff's negligence claim for failure to plead compensable damages in the data breach case); *Walton v. First Merchants Bank*, No. 1:18-cv-01784-JRS-DLP, 2019 WL 826769, at *2 (S.D. Ind. Feb. 20, 2019) (dismissing a negligence claim related to data disclosure because plaintiff "fail[ed] to sufficiently plead any compensable harm related to this incident").

In *Aspen*, the Northern District of Indiana analyzed the plaintiffs' argument that defendant owed a duty to safeguard the public from the risk of data exposure when the defendant allegedly ignored warning signs of a data breach. *Aspen American Ins. Co. v. Blackbaud, Inc.*, 3:22-CV-44 JD, 2023 WL 3737050, *3 (N.D. Ind. May 31, 2023). The court acknowledged that there is not any Indiana caselaw that directly addresses whether there is a common law duty to safeguard private information and relied on the Seventh Circuit's analysis in *Pisciotta* and application of Indiana's Data Breach Notification Statute. *Id.* at *4. The court reasoned that the statute prescribes narrow duties, "'strongly suggest[ing] that Indiana law would not recognize' the common law duty to safeguard private information." *Id.* (quoting *Pisciotta*, 499 F.3d at 637). After reviewing other courts' analysis of the same issue within the Seventh Circuit, the *Aspen* court dismissed the plaintiffs' negligence claim for failing to plausibly allege the duty element.

In *Pisciotta*, plaintiffs brought a class action lawsuit against the defendant-bank that suffered a data breach, alleging they had been harmed by the exposure of their confidential information and incurred costs to protect against potential identity theft. *Pisciotta*, 499 F.3d at 632. In determining whether the fear of future harm constituted a cognizable harm for plaintiffs' negligence claim, the Seventh Circuit analyzed the language set forth in Indiana's Data Breach Notification statute, concluding that Indiana law would not recognize costs spent on credit monitoring as compensable damages. *Id.* at 637.[2] The plaintiffs also alleged they suffered injury when their information was accessed by unauthorized individuals, but the court reasoned the plaintiffs were essentially seeking "to be reimbursed for their efforts to guard against some future, anticipated harm." *Id.* at 638. In reaching its conclusion, the court relied on language from the

[2] When analyzing Indiana's Data Breach Notification statute, the Seventh Circuit reasoned that the statute requires "only that a database owner disclose a security breach to potentially affected consumers" and "do[es] not require the database owner to take any other affirmative act in the wake of a breach." *Pisciotta*, 499 F.3d at 637 (citing to I.C. § 24-4.9, *et seq.*).

Indiana Supreme Court in a toxic tort lawsuit, which explained that "compensable damage requires more than exposure to a future potential harm." *Id.* at 638 – 639. The Seventh Circuit applied that reasoning to *Pisciotta*, concluding plaintiffs' speculative fear of future damages were not compensable under Indiana law. *Id*. at 640.

Here, Plaintiffs do not properly plead that Defendant owed them a duty or that they suffered any cognizable injury and failed to provide proof of actual loss or damages stemming from the Data Security Incident. Plaintiffs' asserted injuries are boilerplate and speculative allegations premised on potential future harm, mitigation efforts to avoid identity theft, and loss in value to their personal information. Amended Compl. ¶ 126 – 128. Plaintiffs do not allege there is any ongoing, present harm, such as fraudulent bank account transactions or non-reimbursed fraudulent charges resulting from Defendant's alleged negligence. Instead, Plaintiffs rely on the risk of future harm in lieu of any actual injury. *Id.* at ¶ 126.

In data breach cases across the country, courts have routinely rejected similar speculative damages allegations when set forth as a basis for injury in negligence claims. *See In re SuperValu, Inc. Customer Data Sec. Breach Litig.*, No. 14-2586, 2018 WL 1189327, at *13 (D. Minn. Mar. 7, 2018) (dismissing negligence claim where "time spent monitoring his account information to guard against potential fraud" was not a "cognizable injury"); *Paul v. Providence Health System-Oregon*, 273 P.3d 106, 110 (Or. 2012) (holding that the threat of future harm to credit or well-being is insufficient as an allegation of damages for a negligence claim); *Reilly v. Ceridien Corp.*, No 10-5142, 2011 WL 735512, *4-5 (D.N.J. Feb 22, 2011) (holding that plaintiff's allegations of a "threat of future injury" were insufficient to establish a compensable injury).

As such, Plaintiffs have failed to state a cause of action for negligence under Indiana law and this claim should be dismissed with prejudice.

b. Plaintiffs' Negligence Claim is Barred by the Economic Loss Rule

Plaintiffs' negligence claim is also barred by the economic loss rule. The economic loss doctrine prohibits recovery in tort for purely economic losses in the absence of personal injury or property damage. *Indianapolis-Marion Cnty. Public Library v. Charlier Clark & Linard, P.C.*, 929 N.E.2d 722, 729 (Ind. 2010). Several federal courts have employed the economic loss doctrine to bar negligence claims in data breach cases where plaintiffs sought purely economic damages. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1172 (D. Minn. 2014) (dismissing negligence claims under law of Alaska, California, District of Columbia, Georgia, Idaho, Illinois, Iowa, Massachusetts, New Hampshire, and New York); *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 761 (C.D. Ill. 2020) (finding that plaintiff's alleged injuries of "lost time and an inability to use or access funds due to a data breach are economic losses"); *see also In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 178 (3d Cir. 2008). Here, Plaintiffs seek economic damages for alleged expenses incurred from the Data Security Incident. Amended Compl. ¶¶ 60 – 62, 126 – 128. The economic loss rule bars such recovery, and this provides an independence basis for dismissal of the claim.

2. Plaintiffs Fail to State a Claim for Negligence *Per Se*

In Indiana, negligence *per se* is the "unexcused or unjustified violation of a duty prescribed by statute." *Brown v. City of Valparaiso*, 67 N.E.3d 652, 656 (Ind. Ct. App. 2016). To establish a valid negligence *per se* claim under Indiana law, a plaintiff must demonstrate the statute protects (1) the class of persons, including plaintiff, (2) against the type of harm which the statute is designed to protect against. *Stachowski v. Estate of Radman*, 95 N.E.3d 542, 544 (Ind. Ct. App. 2015). Indiana law also requires a plaintiff to establish proximate cause to bring a negligence *per*

se claim. *McBride ex rel. Estate of McBride v. Cole Associates, Inc.*, 753 N.E.2d 730, 739 (Ind. Ct. App. 2001) ("negligence *per se* does not mean liability *per se*, that is, a violation of a statutory duty is not actionable negligence unless it was also the proximate cause of the injury").

Plaintiffs' negligence *per se* claim is based on Defendant's alleged violations of Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Amended Compl. ¶¶ 130 – 138. Plaintiffs claim that the unauthorized disclosure of their information violated the FTC Act and caused them injury. *Id.* However, Plaintiffs have not pled any facts to establish proximate cause or shown that they have incurred any actual damages as a result of Defendant's alleged statutory violations.

Courts in this district have consistently concluded that the FTC Act does not create a private right of action for individuals. *Merriam v. GC Services*, No. 1:18-cv-80, 2018 WL 3068857, *1 (N.D. Ind. June 21, 2018) (determining no private right of action exists under the FTC Act); *Norman v. Ally Financial Bank*, No. 2:20-CV-51-JVB-JEM, 2021 WL 26300, at *2 (N.D. Ind. Jan. 4, 2021) (reasoning that no private right of action exists under the FTC Act and noting that only the FTC can bring a lawsuit to enforce the FTC Act). The *Merriam* opinion is consistent with caselaw from across the country wherein courts have consistently rejected negligence *per se* claims based on violations of the FTC Act because the FTC Act does not provide for a private right of action. *See Morrison v. Back Yard Burgers, Inc.*, 91 F.3d 1184, 1187 (8th Cir. 1996) (holding that the FTC Act does not provide for a private right of action); *Marshall v. Conway Regional Medical Center*, No. 4:20-CV-00933 JM, 2020 WL 5746839, at *2 (E.D. Ark. Sept. 25, 2020) (determining the FTC Act does not permit a private right of action in class action data breach lawsuit); *U.S. v. Philip Morris, Inc.*, 263 F.Supp.2d 72, 78 (D.D.C. 2003) ("The FTC Act is enforced exclusively by the FTC; there is no private right of action under the statute").

Additionally, in *Holloway v. Bristol–Myers Corp.*, 485 F.2d 986 (D.C. Cir. 1973), the court held that private actions under the FTC Act could not be maintained. After outlining the threat to government's enforcement efforts if private actions were involved, the *Holloway* court concluded that "a private right of action to enforce the Federal Trade Commission Act—however desirable or logical this might appear in the abstract—would be contrary to the legislative design which we discern to have been deliberately wrought." *Id.* at 1002. The seminal *Holloway* decision has been adopted by courts within the Seventh Circuit. *See Merriam*, 2018 WL 3068857, *1; *Norman*, 2021 WL 26300, at *2; *Int'l Tax Advisors, Inc. v. Tax Law Associates, LLC*, No. 08-C-2222, 2011 WL 612093, at *5 (N.D. Ill. Feb. 15, 2011).

While Plaintiffs try to rely on alleged violations of the FTC Act to support their negligence *per se* claim, the statute itself is not independently actionable. Plaintiffs' Amended Complaint is an attempt to do an end around the clearly established lack of such a private action. They assert only that Defendant has generally (allegedly) violated the FTC Act and therefore should be held liable. This is nothing more than a direct action under the Act in disguise. Plaintiffs' attempts should be rejected. Further, Plaintiffs have not pled any facts showing proximate cause or that they suffered any cognizable damages from any of Defendant's alleged violations of the FTC Act. Accordingly, Plaintiffs' negligence *per se* claim should be dismissed for failure to state a claim.

3. Plaintiffs Fail to State a Claim for Breach of Implied Contract

To bring a breach of contract action under Indiana law, a plaintiff must establish (1) a contract existed, (2) the defendant breached the contract, and (3) the plaintiff suffered damage as a result of defendant's breach. *Trustees of Indiana University v. Spiegell*, 186 N.E.3d 1151, 1158 (Ind. Ct. App. 2022). The elements of an implied-in-fact contract are the same as an express contract: offer, acceptance, and consideration, but the parties' conduct expresses the agreement.

Garwood Packaging, Inc. v. Allen & Co., Inc., IP 98-1058-C-M/S, 2002 WL 31924512, at *19 (S.D. Ind. Dec. 26, 2002). In Indiana, an implied contract "arises out of acts and conduct of the parties, coupled with a meeting of the minds and a clear intent of the parties in the agreement." *Nationwide Ins. Co. v. Heck*, 873 N.E.2d 190, 197 n1 (Ind. Ct. App. 2007).

In *Archey*, the plaintiff sued claiming he was injured by the exposure of his personal information after the defendant suffered a cyberattack. *Archey v. Osmose Utilities Services, Inc.*, No. 20-cv-05247, 2021 WL 3367156 (N.D. Ill. Aug. 3, 2021). The plaintiff claimed defendant breached an implied contract between the parties by failing to protect his personal information and failing to timely notify him of the data breach, but the plaintiff failed to plead any actual loss or injury from the exposure of his information. *Id*. at *2. The Northern District of Illinois dismissed the plaintiff's breach of implied contract claim for failure to state a claim because the plaintiff did not plead any damages. *Id*.

Here, Plaintiffs allege Defendant entered into implied contracts with them through their credit union or that the Plaintiffs were third-party beneficiaries of their credit unions' contracts with Defendant, that Defendant agreed to protect and not disclose their PII and agreed to timely notify them of any data breach, and Plaintiffs suffered injury. Amended Compl. ¶¶ 140 – 157.

Plaintiffs are unable to point to any facts establishing a valid implied contract between themselves and Defendant, or a valid third-party beneficiary claim between them, their credit union, and Defendant. Specifically, Plaintiffs fail to assert any allegations that establish mutual assent or clear intent between the parties, rendering it impossible for any enforceable implied contract or third-party beneficiary claim to exist between Plaintiffs, their credit unions, and Defendant. Without a meeting of the minds, there is no enforceable contract. Further, Plaintiffs

Amended Complaint does not allege any intent by Defendant to enter into implied or third-party beneficiary contracts.

Finally, Plaintiffs' breach of implied contract claim fails to allege that Plaintiffs suffered any compensable damages beyond the mere future risk of injury. Like the plaintiff in *Archey*, Plaintiffs have not suffered any actual harm stemming from the Data Security Incident. Having failed to allege a meeting of the minds, mutual assent between the parties, or any valid form of damages, Plaintiffs fail to state a claim for breach of implied contract and this claim must be dismissed.

4. Plaintiffs Fail to State a Claim for Invasion of Privacy

Indiana recognizes four different types of invasion of privacy: (1) intrusion upon seclusion; (2) appropriation of likeness; (3) public disclosure of private facts; and (4) false-light publicity. *Community Health Network, Inc. v. McKenzie*, 185 N.E.3d 368, 380 (Ind. 2022). Plaintiffs frame their invasion of privacy under an intrusion upon seclusion theory. Amended Compl. ¶¶ 159 – 171. To bring a claim for invasion of privacy by intrusion upon a person's seclusion under Indiana law, a plaintiff must show (1) a purposeful or intentional intrusion that (2) is highly offensive to a reasonable person. *Curry v. Whitaker*, 943 N.E.2d 354, 358 (Ind. Ct. App. 2011). The Indiana Supreme Court has narrowly construed an invasion of privacy claim by requiring the "intrusion into the plaintiff's private 'physical' space." *Id.* (quoting *Cullison v. Medley*, 570 N.E.2d 27, 31 (Ind. 1991)). *Curry* notes that there are no Indiana cases where an intrusion upon seclusion claim was established "without physical contact or invasion of the plaintiff's physical space…" *Id.* Indiana caselaw continues to uphold this narrow application.

Plaintiffs allege simply that they had a reasonable expectation of privacy in their information, but not that anyone invaded their own physical space. Amended Compl. ¶¶ 159 –

171.146 – 158. Plaintiffs' Amended Complaint attempts to create the impression that the Data Security Incident constitutes an intentional inference with Plaintiffs' solitude or seclusion, but at the same time their own statements establish that any "intrusion" was committed by a criminal third-party into Defendant's own private space. *Id*. at ¶¶ 3 – 5, 167 – 168. Furthermore, the Plaintiffs can only proffer conclusory allegations that Defendant somehow "acted with a knowing state of mind" a to intruding into Plaintiff's seclusion when it suffered a cyberattack of its own systems. *Id*. at ¶¶ 164 – 165151.

This, based on Plaintiffs' own allegations, they have failed to allege sufficient facts to support a claim for intrusion upon seclusion under Indiana law. Indiana caselaw is clear that to prevail on an intrusion upon seclusion cause of action, there must be a physical intrusion into a person's "physical space" that is "highly offensive to a reasonable person." *Curry*, 943 N.E.2d at 358. Plaintiffs' allegations center on the theft of intangible personal data stored on Defendant's computer systems and perpetrated by a third-party criminal – there was no physical contact or invasion of either of the Plaintiffs' physical space by Defendant. Accordingly, Plaintiffs' intrusion upon seclusion claim should be dismissed for failure to state a claim.

5. Plaintiffs Fail to State a Claim for Unjust Enrichment

Indiana law requires three elements to bring an unjust enrichment claim: "(1) a benefit conferred upon another at the express or implied request of this other party; (2) allowing the other party to retain the benefit without restitution would be unjust; and (3) the plaintiff expected payment." *Woodruff v. Ind. Family & Soc. Servs. Admin.*, 964 N.E.2d 784, 791 (Ind. 2012). "Put another way, 'a plaintiff must establish that a measurable benefit has been conferred on the defendant under such circumstances that the defendant's retention of the benefit without payment

would be unjust. One who labors without an expectation of payment cannot recover in quasi-contract.'" *Id*.

When faced with similar allegations in a case against a restaurant chain, the Central District of Illinois dismissed the unjust enrichment claim, noting that the plaintiff "paid for food products. She did not pay for a side order of data security and protection; it was merely incident to her food purchase." *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016); *see also Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 766 (C.D. Ill. 2020) (dismissing unjust enrichment claim where "Plaintiffs have not alleged that any specific portion of their payments went toward data protection; rather, they state that their payments were for food and gas"); *In re SuperValu, Inc.*, 925 F.3d 955, 966 (8th Cir. 2019) ("Because [plaintiff] does not allege that any specific portion of his payment went toward data protection, he has not alleged a benefit conferred in exchange for protection of his personal information nor has he shown how SuperValu's retention of his payment would be inequitable."); *In re Arthur J. Gallagher Data Breach Litig.*, No. 22-137, 2022 WL 4535092, at *10 (N.D. Ill. Sept. 28, 2022) (dismissing unjust enrichment claim brought by clients and employees following data breach because plaintiff did not plausibly allege defendant retained any benefit).

Here, Plaintiffs allege they "conferred a benefit upon Defendant" in the form of their PII and payment, that Defendant accepted, retained, and profited from that benefit, and Defendant was unjustly enriched by saving costs it reasonably should have expended on data security measures to secure PII. Amended Compl. ¶¶ 173 – 181. However, Plaintiffs concede they did not have any direct relationship with Defenant and seem to indicate they did were not even aware of Defendant prior to being notified of the incident. *See, e.g.* Amended Compl. ¶ 47 (alleging that Defendant contracted with Webster's credit union only upon "information and belief"). As a result, Plaintiffs

simply do not (and could not) allege they conferred some benefit to Defendant at its request. Their boilerplate assertion that they conferred a benefit on Defendant because "[a]fter all" it "benefitted from using their PII" does not meet this element. Moreover, they do not claim in even conclusory terms that they somehow expected payment from anyone at all, let alone ***Defendant*** – with whom, again, they had no relationship. Plaintiff's allegations that they somehow expected Defendant to "provid[e] a reasonable level of security" have nothing to do with laboring with the expectation of payment, and do not meet the elements of an unjust enrichment claim under Indiana law.

Put simply, Plaintiffs did not confer any benefits upon Defendant at its request, did not expect any kind of payment, and have not established anything "unjust," Plaintiffs' unjust enrichment claim should be dismissed with prejudice.

6. Plaintiffs Fail to State a Claim for Bailment

In Indiana, a bailment cause of action arises when: (1) personal property belonging to a bailor is delivered into the exclusive possession of the bailee, and (2) the property is accepted by the bailee. *Winters v. Pike*, 171 N.E.3d 690, 699 (Ind. Ct. App. 2021) (quoting *Cox v. Stoughton Trailers, Inc.*, 837 N.E.2d 1075, 1082 (Ind. Ct. App. 2005)). For delivery to occur in a bailment relationship, there must be a full transfer of the property, either actually or constructively, to the sole custody of the bailee to the exclusion of both the owner of the property and others. *See Winters*, 171 N.E.3d at 699. If a bailment is found to exist, the bailee in possession of the bailed property must exercise the degree of care commensurate with the benefit derived from the arrangement. *Id*.

Albanese Confectionary involved an employer firing the employee plaintiff and remotely wiping the employee's personal smartphone, resulting in the loss of personal data. *Albanese Confectionery Grp., Inc. v. Cwik*, 165 N.E.3d 139 (Ind. Ct. App. 2021). The terminated employee

brought a bailment claim, arguing that the employer's control over her smartphone constituted a bailment relationship. *Id.* at 148. The court denied the plaintiff's argument, reasoning that the employer never had exclusive control over the smartphone data because both the plaintiff and employer could access the smartphone. *Id.*

Following that exact logic, Plaintiffs' bailment cause of action here fails because Defendant never had exclusive control over Plaintiffs' information. Plaintiffs assert that they entrusted their information to Defendant through their credit unions, who then shared this information with Defendant, that Defendant had exclusive possession of the information, and Plaintiffs incurred damages through the misuse of their information. Amended Compl. ¶¶ 3, 16, 23 – 28, 183 – 190. During the time that Plaintiffs' credit unions and Defendant had access to Plaintiffs' information, Plaintiffs were and are still at full liberty to utilize their personal information for their own purposes. For example, Plaintiffs still had complete access to use their Social Security numbers – whether they wanted to open an additional bank account, apply for a mortgage, or enroll in Medicare – Plaintiffs do not claim they were precluded from taking any of these actions by Defendant's possession of a copy of some information about them. Furthermore, both the credit unions, Plaintiffs, and Defendant had access to the information – no entity or individual had exclusive control over it. Any assertion to the contrary would be absurd. Indeed, Plaintiffs' own claims would collapse if that were the case – they allege that Defendant still has possession of their personal information, yet at the same time, they assert the same information is at risk of malicious use by unknown third parties. At no point did Defendant have exclusive control over either the Plaintiffs' information to the exclusion of all others.

As such, Plaintiffs have failed to state a claim for bailment and this cause of action should be dismissed with prejudice.

C. Alternatively, Immaterial and Impertinent Allegations Should be Stricken.

If the Court does not dismiss Plaintiffs' Amended Class Action Complaint in its entirety, the numerous immaterial and impertinent allegations concerning identity theft, statistics about cybercrime, and generic business best practices that have nothing to do with the parties or facts of this case should be struck from the complaint.

Federal Rule of Civil Procedure 12(f) permits a court to strike immaterial and impertinent allegations from a pleading on its own or upon motion by a party. A motion to strike under Rule 12(f) should be granted when "the language in the pleading at issue has no possible relation to the controversy and is clearly prejudicial." *Mitchell v. Bendix Corp*., 603 F. Supp. 920, 921 (N.D. Ind. 1985).

Instead of focusing solely on the relevant Data Security Incident and Plaintiffs' individual allegations, Plaintiffs added extraneous material concerning the actions of identity thieves, statistics about cybercrime, and generic best practices for businesses. Amended Compl. ¶¶ 75 – 97. Plaintiffs pled no actual facts regarding the motivations of the cybercriminals who perpetrated the attack on Defendant beyond conclusory and speculative allegations. To make up for that missing information, Plaintiffs include immaterial and generalized allegations that are designed to improperly inflame the issues and lend weight to the alleged risk of future identity theft. Plaintiffs' Amended Complaint should be limited to the criminal Data Security Incident and their individual experiences, and this Court should strike paragraphs 75 – 97 pursuant to Rule 12(f).

IV. Conclusion

For all the foregoing reasons, Defendant Bradford-Scott d/b/a Sharetec respectfully requests that the Plaintiffs' Amended Complaint be dismissed in its entirety with prejudice pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). In the event the Court does

not dismiss the Amended Complaint in its entirety, Defendant respectfully requests that it strike paragraphs 75 – 97 from the Amended Complaint pursuant to Federal Rule of Civil Procedure 12(f).

Date: June 5, 2024

By: *Claudia McCarron*
MULLEN COUGHLIN LLC
Claudia McCarron
Michael Jervis*
Kayleigh Watson*
426 W. Lancaster Avenue
Suite 200
Devon, PA 19333
Tel: (267) 930-4498
Email: cmccarron@mullen.law
mjervis@mullen.law
kwatson@mullen.law

Attorneys for Defendant Bradford-Scott

**Admitted Pro Hac Vice*

CERTIFICATE OF SERVICE

I hereby certify that on June 5, 2024, the foregoing was electronically filed with the Clerk of Court using the CM/ECF system which will send notification of such filing to all counsel of record.

By: */s/ Claudia McCarron*